

1 MAYER BROWN LLP
ANDREW JOHN PINCUS (*Pro Hac Vice*)
2 apincus@mayerbrown.com
1999 K Street, NW
3 Washington, DC 20006
Tel: (202) 263-3220 / Fax: (202) 263-3300

4 MAYER BROWN LLP
LEE H. RUBIN (SBN 141331)
5 lrubin@mayerbrown.com
DONALD M. FALK (SBN 150256)
6 dfalk@mayerbrown.com
SAMANTHA C. BOOTH (SBN 298852)
7 sbooth@mayerbrown.com
Two Palo Alto Square, Suite 300
8 3000 El Camino Real
9 Palo Alto, CA 94306-2112
Tel: (650) 331-2000 / Fax: (650) 331-2060

10 *Attorneys for Plaintiff Twitter, Inc.*

11 **UNITED STATES DISTRICT COURT**
12 **NORTHERN DISTRICT OF CALIFORNIA**
13 **OAKLAND DIVISION**

14 TWITTER, INC.,

15
16 Plaintiff,

17 v.

18
19 WILLIAM P. BARR, Attorney General of the
United States, *et al.*,

20
21 Defendants.
22
23
24
25
26
27
28

Case No. 14-cv-4480-YGR

**TWITTER, INC.'S OPPOSITION TO
DEFENDANTS' INVOCATION OF
STATE SECRETS AND MOTION TO
DISMISS**

Date: June 4, 2019

Time: 2:00 p.m.

Courtroom 1, Fourth Floor

Judge: Hon. Yvonne Gonzalez Rogers

TABLE OF CONTENTS

	<u>Page</u>
INTRODUCTION	1
ARGUMENT	3
A. The Government Has Not Shown that the Classified Declaration Meets the Exceptionally High Standard Necessary to Qualify as a State Secret	3
1. The Government’s privilege assertion requires searching judicial scrutiny.....	4
2. The public record provides ample reason to believe that the Classified Declaration is not a State Secret	6
3. The Ninth Circuit has repeatedly held that mere classification does not render information a state secret.....	10
4. The Government relies on categorical—and insupportable— assumptions regarding the risk of national security harm associated with granting Twitter’s cleared counsel access to the Classified Declaration.....	11
B. Dismissal Is Not Warranted Even if Some Portions of the Classified Declaration Qualify as State Secrets.....	17
1. The FISA and NSL statutes reflect a Congressional intent to provide a judicial forum for challenges to restrictions on aggregate disclosure of national security process	17
2. Dismissal also is not warranted here because a finding of state secrets would not deprive Defendants of a <i>valid</i> defense	20
3. Ample mitigation measures are available here to protect any state secrets.....	20
CONCLUSION.....	21

TABLE OF AUTHORITIES**Page(s)****Cases**

<i>ACLU v. Brown</i> , 619 F.2d 1170 (7th Cir. 1980)	4
<i>Al Haramain Islamic Found., Inc. v. U.S. Dep't of Treasury</i> , 686 F.3d 965 (9th Cir. 2012)	2, 14, 15, 16
<i>Al-Haramain Islamic Found., Inc. v. Bush</i> , 507 F.3d 1190 (9th Cir. 2007)	17
<i>Am.-Arab Anti-Discrimination Comm. v. Reno</i> , 70 F.3d 1045 (9th Cir. 1995)	16, 20
<i>Doe v. Gonzales</i> , 386 F. Supp. 2d. 66 (D. Conn. 2005)	9
<i>Doe, Inc. v. Mukasey</i> , 549 F.3d 861 (2d Cir. 2008)	3, 9
<i>El-Masri v. United States</i> , 479 F.3d 296 (4th Cir. 2007)	15
<i>Ellsberg v. Mitchell</i> , 709 F.2d 51 (D.C. Cir. 1983)	4, 5, 15
<i>Emory v. Sec'y of Navy</i> , 819 F.2d 291 (D.C. Cir. 1987)	6
<i>Fazaga v. FBI</i> , 916 F.3d 1202 (9th Cir. 2019)	<i>passim</i>
<i>Gen. Dynamics Corp. v. United States</i> , 563 U.S. 478 (2011)	17
<i>Halkin v. Helms</i> , 598 F.2d 1 (D.C. Cir. 1978)	5, 15
<i>Halpern v. United States</i> 258 F.2d 36 (2d Cir. 1958)	14
<i>Hamdi v. Rumsfeld</i> , 542 U.S. 507 (2004)	6
<i>Hassan v. City of New York</i> , 804 F.3d 277 (3d Cir. 2015)	6

1	<i>Hepting v. AT&T Corp.</i> ,	
	439 F. Supp. 2d 974 (N.D. Cal. 2006)	9
2	<i>Horn v. Huddle</i> ,	
3	647 F. Supp. 2d 55 (D.D.C. 2009)	12
4	<i>Kinoy v. Mitchell</i> ,	
5	67 F.R.D. 1 (S.D.N.Y. 1975)	15
6	<i>Loral Corp. v. McDonnell Douglas Corp.</i>	
	558 F.2d 1130 (2d Cir. 1977)	14
7	<i>Mohamed v. Jeppesen DataPlan, Inc.</i> ,	
8	614 F.3d 1070 (9th Cir. 2010)	<i>passim</i>
9	<i>In re Nat'l Sec. Agency Telecomms. Records Litig.</i> ,	
10	595 F. Supp. 2d 1077 (N.D. Cal. 2009)	12
11	<i>In re NSL</i> ,	
	863 F.3d 1110 (9th Cir. 2017)	3, 6, 8, 9
12	<i>In re Sealed Case</i> ,	
13	494 F.3d 139 (D.C. Cir. 2007)	13, 21
14	<i>In re U.S.</i> ,	
15	872 F.2d 472 (D.C. Cir. 1989)	3, 7, 21
16	<i>In re Under Seal</i> ,	
	945 F.2d 1285 (4th Cir. 1991)	5
17	<i>Sterling v. Constantin</i> ,	
18	287 U.S. 378 (1932)	6, 15
19	<i>Sterling v. Tenet</i> ,	
20	416 F.3d 338 (4th Cir. 2005)	15
21	<i>Stillman v. CIA</i> ,	
	319 F.3d 546 (D.C. Cir. 2003)	3
22	<i>Tenet v. Doe</i> ,	
23	544 U.S. 1 (2005)	6
24	<i>Unigard Sec. Ins. Co. v. Lakewood Eng'g & Mfg. Corp.</i> ,	
25	982 F.2d 363 (9th Cir. 1992)	12
26	<i>United States v. Ahmad</i> ,	
	499 F.2d 851 (3d Cir. 1974)	8
27	<i>United States v. Nixon</i> ,	
28	418 U.S. 683 (1974)	5

1	<i>United States v. Reynolds</i> ,	
2	345 U.S. 1 (1953).....	<i>passim</i>
3	<i>Washington v. Trump</i> ,	
4	847 F.3d 1151 (9th Cir. 2017)	6
5	<i>Webster v. Doe</i> ,	
6	486 U.S. 592 (1988).....	6, 7, 14
7	Statutes	
8	5 U.S.C. § 552.....	11
9	18 U.S.C. App. 3.	2, 13
10	18 U.S.C. § 3511	18, 19
11	50 U.S.C. § 1806(f).....	2, 16, 17, 18
12	50 U.S.C. § 1861	8, 18
13	Other Authorities	
14	26 Charles Alan Wright et al., Fed. Prac. & Proc. Evid. § 5663 (2019).....	6
15	Executive Order 13526	10
16	Robert M. Pallito & William G. Weaver, Presidential Secrecy and the Law 86, 90	
17	(2007).....	5, 6
18	Termination Procedures for National Security Letter Nondisclosure Requirement,	
19	Fed. Bureau of Investigation (Nov. 24, 2015), https://www.fbi.gov/file-	
20	repository/nsi-ndp-procedures.pdf	8
21		
22		
23		
24		
25		
26		
27		
28		

INTRODUCTION

More than two years after the Government voluntarily introduced the Classified Steinbach Declaration (“Classified Declaration”) into evidence to support its motion for summary judgment, it asserts that the same declaration is “a state secret” and must be removed from the case. Yet it does not stop there: The Government maintains that the entire case must now be dismissed as a result. All that has changed is the Government’s tactical convenience. The Government wanted the Classified Declaration in evidence when it could help the Government, but belatedly insists that the same document is a state secret now that the litigating calculus has changed.

The Government cites no case (and Twitter is aware of none) where it has asserted that the state secrets privilege requires removal of evidence that the Government itself introduced into the case. No wonder; the Government’s position cannot be right. To uphold the Government’s state secrets determination, the Court would have to agree that the Classified Declaration cannot be maintained in evidence (even under seal) without posing an unjustifiable risk to national security, yet the declaration has been in evidence for more than two years without any inkling of harm.

Neither can it be true—as the Government now insists—that no private counsel in a civil case can be entrusted with access to national security information *under any circumstance*. Private cleared counsel have had access to classified information in both criminal and civil matters without posing a threat to the national security. And the Court has a broad array of protective tools—including the ability to hold *in camera* hearings with only cleared persons present—to address any factual disputes regarding the Classified Declaration. The narrow question presented here is whether Twitter’s cleared counsel’s access to the contents of *this* Classified Declaration represents an intolerable risk to national security. On that point, the Government is silent. The Government’s Motion loses sight of the purpose and scope of the state secrets privilege. The Government invokes the privilege based on the “imminent[.]” risk that “the Court ... may ... enter an order of disclosure” of the Classified Declaration to cleared counsel, Dkt. No. 281, at 22—not because of the sensitivity of the information in the document.

1 But the state secrets privilege is a national-security safeguard, not a litigation weapon. As a
2 matter of law, the privilege cannot hinge on whether the Court would otherwise grant cleared
3 counsel access to the Classified Declaration. That decision whether to grant access rests with
4 Article III courts. *See Al Haramain Islamic Found., Inc. v. U.S. Dep’t of Treasury*, 686 F.3d
5 965, 983 (9th Cir. 2012) (“*Al-Haramain II*”); 50 U.S.C. § 1806(f) (FISA); 18 U.S.C. App. 3, § 1
6 *et seq.* (CIPA). Just as the Government cannot supplant this Court’s authority to manage
7 discovery by unilaterally declaring that Twitter’s cleared counsel has no “need to know” the
8 information in the Classified Declaration, the Government cannot accomplish the same result by
9 threatening a state secret designation unless it gets its way. *See* Twitter’s Opp. to Gov’t
10 Response to OSC, Dkt. No. 265, at 5–12.

11 The Government’s state secret designation also effectively equates the state secrets
12 privilege with classification. Ninth Circuit law is clear that it cannot do so. *See Fazaga v. FBI*,
13 916 F.3d 1202, 1227 (9th Cir. 2019). And the public record provides strong reasons to doubt
14 that the Classified Declaration meets the higher standard for a state secret: The Court described
15 the Classified Declaration as containing “generic” and “boilerplate” discussions of the mosaic
16 theory and “broad brush” concerns about the risks of aggregate reporting. Those items sound
17 nothing like state secrets. Moreover, the information in that 2016 Declaration relates to the
18 volume of national security process that Twitter received back in 2013.

19 The Government’s overreach is exemplified by its new-found insistence that *any*
20 information about Twitter’s receipt of national security process—including whether Twitter has
21 *ever* received FISA process—is a “state secret.” The Court already rejected that argument, and
22 the public is already aware that Twitter receives national security process. The Government has
23 not explained—nor can it—how information in the public domain now qualifies as a state secret.

24 The Government’s state secrets claim should be rejected in full. Even if the Court were
25 to conclude that Twitter’s cleared counsel should not see some or all of the Classified
26 Declaration, the proper consequence would be redaction of the sensitive information or denial of
27 Twitter’s access request under the Court’s broad discovery powers. The document should not be
28 removed from evidence.

Under no circumstances is dismissal appropriate. As the Government admits (in urging this Court to follow *Stillman v. CIA*, 319 F.3d 546 (D.C. Cir. 2003)), courts have routinely resolved disputes over nondisclosure obligations. *See, e.g., In re NSL*, 863 F.3d 1110, 1119–20 (9th Cir. 2017); *Doe, Inc. v. Mukasey*, 549 F.3d 861, 864 (2d Cir. 2008). Nor could dismissal be squared with the FISA and NSL regimes, which reflect a Congressional determination that challenges to nondisclosure obligations are justiciable, and that available procedural mechanisms suffice to protect the Government’s national security interests. Dismissal is also inappropriate because the Court has already held that the Classified Declaration does not provide the Government a “valid defense” to Twitter’s claims, *i.e.*, one that “is meritorious ... and would require judgment for the defendant.” *Fazaga*, 916 F.3d at 1253. That precludes dismissal even if the Classified Declaration were removed from evidence.

ARGUMENT

A. The Government Has Not Shown that the Classified Declaration Meets the Exceptionally High Standard Necessary to Qualify as a State Secret.

The Government misconceives what qualifies as a “state secret.” The Government must show that any use of the allegedly privileged evidence in a particular case—even subject to procedural safeguards—would create so great a “danger ... [of] expos[ing] military secrets which, in the interest of national security, should not be divulged,” *United States v. Reynolds*, 345 U.S. 1, 10 (1953), that the evidence must be altogether “remove[d] ... from the litigation,” *Mohamed v. Jeppesen DataPlan, Inc.*, 614 F.3d 1070, 1079 (9th Cir. 2010).

Given these “draconian” consequences, *In re U.S.*, 872 F.2d 472, 477 (D.C. Cir. 1989), the privilege must be reserved for those “exceptional circumstances,” *Jeppesen*, 614 F.3d at 1077, in which no procedural safeguards could adequately guard against the risk of inadvertent disclosure and resultant harm to national security. “[S]imply saying ‘military secret,’ ‘national security’ or ‘terrorist threat’ or invoking an ethereal fear that disclosure will threaten our nation is insufficient to support the privilege.” *Fazaga*, 916 F.3d at 1227 (quoting *Al-Haramain Islamic Found., Inc. v. Bush*, 507 F.3d 1190, 1203 (9th Cir. 2007) (“*Al-Haramain I*”). Likewise, the mere fact that information is classified is not enough. *Id.* at 1227; *Jeppesen*, 614 F.3d at 1082.

1 The Government has not carried its burden of showing exceptional circumstances here.
 2 Even the limited public record reveals that the Government's state secret privilege claim cannot
 3 withstand the searching judicial scrutiny required under governing law.

4 **1. The Government's privilege assertion requires searching judicial scrutiny.**

5 Both the Supreme Court and the Ninth Circuit have emphasized courts' obligation to
 6 "make an independent determination," *Jeppesen*, 614 F.3d at 1080, as to whether, "in light of 'all
 7 the circumstances of the case,' the Government has shown 'a reasonable danger that compulsion
 8 of the evidence [in the case] will expose ... matters which, in the interest of national security,
 9 should not be divulged,'" *id.* at 1081 (quoting *Reynolds*, 345 U.S. at 10). The Court must assure
 10 itself "that the state secrets privilege is asserted no more frequently and sweepingly than
 11 necessary." *Fazaga*, 916 F.3d at 1228 (quoting *Jeppesen*, 614 F.3d at 1082).

12 Though the Executive is obviously entitled to a degree of deference on matters of foreign
 13 policy and national security, courts have long recognized that its institutional habit and
 14 inclination will tilt the balance excessively against disclosure. *See Ellsberg v. Mitchell*, 709 F.2d
 15 51, 58 (D.C. Cir. 1983). The Court therefore should "not accept at face value the government's
 16 claim or justification of privilege," but has an obligation to review the Government's
 17 submissions with "a very careful, indeed a skeptical eye." *Jeppesen*, 614 F.3d at 1082.

18 In addition, "the more compelling a litigant's showing of need for the information in
 19 question, the deeper 'the court should probe in satisfying itself that the occasion for invoking the
 20 privilege is appropriate.'" *Ellsberg*, 709 F.2d at 58–59 (quoting *Reynolds*, 345 U.S. at 11);
 21 *accord ACLU v. Brown*, 619 F.2d 1170, 1173 (7th Cir. 1980) (because appellate court's "in
 22 camera examination of the material" suggested that state secret assertion is "dubious," district
 23 court on remand may reject "formal claim of privilege" if "the material is needed by plaintiffs").

24 Twitter has made a compelling showing of need. The Government has asserted the state
 25 secrets privilege over evidence it voluntarily placed at the "center of this litigation" by insisting
 26 that it compels judgment in its favor. Dkt. No. 281, at 23. A litigant's need for access to the
 27 evidence being used against it is a basic principle of our adversarial system. While this Court
 28

1 has found the Classified Declaration insufficient to support the Government’s restrictions on
2 Twitter’s speech, Twitter is entitled (with appropriate procedural safeguards) to respond to and
3 test the Government’s proffered evidence, both in these proceedings and on appeal. The
4 Government goes so far as to claim that all “[i]nformation regarding national security legal
5 process that has been served on Twitter, including ... the quantity and type of any such process”
6 is a “state secret.” Dkt. No. 281-1, ¶ 4(i). But that information is at the heart of any challenge to
7 a FISA or NSL non-disclosure obligation.

8 Separation-of-powers principles reinforce the need for close scrutiny of the
9 Government’s belated assertion that the Classified Declaration is a state secret. The Government
10 is trying to use the state secrets privilege to foreclose judicial review of colorable constitutional
11 claims of Executive incursion on civil liberties. That use of the state secrets privilege to shield
12 the Government in civil constitutional litigation had not even been contemplated when *Reynolds*
13 was decided or for decades afterward, when the privilege “surfaced only rarely” and mainly in
14 “commercial” disputes with former employees and military contractors. *See Halkin v. Helms*,
15 598 F.2d 1, 14 n.9 (D.C. Cir. 1978) (Bazelon, J., dissenting from denial of reh’g en banc)
16 (observing as much). Since then, however, “the privilege has taken in much greater territory
17 than that original justification contemplated,” and now “obstructs the constitutional duties of
18 courts to oversee executive action.” Robert M. Pallito & William G. Weaver, *Presidential*
19 *Secrecy and the Law* 86, 90 (2007); *id.* at 106 (noting dramatic increase in use of *Reynolds*
20 privilege); *see also In re Under Seal*, 945 F.2d 1285, 1288 (4th Cir. 1991) (noting the “growing
21 number” of state secrets assertions in constitutional cases).

22 And the Government’s suggestion that upholding the state secrets privilege would require
23 dismissal of Twitter’s constitutional claims necessarily strains the Constitution’s substantive and
24 structural protections for civil liberties. As a structural matter, “[o]ur system of government
25 ‘requires that federal courts on occasion interpret the Constitution in a manner at variance with
26 the construction given the document by another branch.’” *United States v. Nixon*, 418 U.S. 683,
27 704 (1974) (quoting *Powell v. McCormack*, 395 U.S. 486, 549 (1969)). Even in matters
28 involving national security, courts routinely “review executive action ... for compliance with the

1 Constitution.” *Washington v. Trump*, 847 F.3d 1151, 1161 (9th Cir. 2017) (rejecting Executive
 2 invocation of absolute discretion in matters of immigration and national security); *Sterling v.*
 3 *Constantin*, 287 U.S. 378, 401 (1932) (“allowable limits of military discretion” raise “judicial
 4 questions.”); *Emory v. Sec’y of Navy*, 819 F.2d 291, 294 (D.C. Cir. 1987) (similar).

5 In upholding the NSL regime, the Ninth Circuit repeatedly invoked the “availability of
 6 judicial review” to recipients of national security process who wished to challenge the
 7 constitutionality of nondisclosure obligations imposed upon them. *In re NSL*, 863 F.3d 1110,
 8 1125–27 (9th Cir. 2017). And “history teaches” that it is precisely where the Government urges
 9 a “most compelling” national security interest that courts “must be most vigilant in protecting
 10 constitutional rights.” *Hassan v. City of New York*, 804 F.3d 277, 306–07 (3d Cir. 2015); *see*
 11 *also Hamdi v. Rumsfeld*, 542 U.S. 507, 532 (2004).

12 To be sure, sufficiently grave national security concerns may outweigh civil liberties and
 13 separation-of-powers concerns in extreme cases.¹ “[T]he Supreme Court has cautioned,”
 14 however, “against ‘precluding review of constitutional claims’ and ‘broadly interpreting
 15 evidentiary privileges.’” *Fazaga*, 916 F.3d at 1253 (quoting *In re Sealed Case*, 494 F.3d 139,
 16 151 (D.C. Cir. 2007)). The rights at stake in this litigation should prompt heightened skepticism
 17 before such privilege claim can be sustained. There is too long a history of Executive misuse
 18 and overuse of secrecy to violate constitutional rights, discredit political enemies, and “conceal
 19 its own errors.” *E.g.*, 26 Charles Alan Wright et al., *Fed. Prac. & Proc. Evid.* § 5663 (2019)
 20 (collecting examples); *accord* Pallito & Weaver, *supra*, at 86, 90.

21 **2. The public record provides ample reason to believe that the Classified** 22 **Declaration is not a State Secret.**

23 Though Twitter cannot know the contents of the Classified Declaration, the public record

24 ¹ Thus, the Supreme Court has held that the state secrets privilege may bar constitutional claims
 25 “against the Government based on covert espionage agreements.” *Tenet v. Doe*, 544 U.S. 1, 3
 26 (2005). But the Court underscored the narrowness of its ruling by distinguishing *Webster v. Doe*,
 27 486 U.S. 592 (1988), where the court observed that the “den[ial of] any judicial forum for a
 28 colorable constitutional claim” would present a “serious constitutional question.” *Id.* at 603.
 The *Tenet* Court perceived a significant “difference, for purposes of *Totten*, between a suit
 brought by an acknowledged (though covert) employee of the CIA [as in *Webster*] and one filed
 by an alleged former spy.” *Tenet*, 544 U.S. at 10.

1 provides many reasons to doubt that any genuine “state secret” appears in the Government’s
2 explanation of why it redacted the precise amount of national security process Twitter received
3 over six years ago. The Court described the Classified Declaration as containing essentially
4 “generic” and “boilerplate” discussions of the mosaic theory and “broad brush” concerns about
5 the risks of aggregate reporting as Twitter has proposed. Dkt. No. 172 at 18; Dkt. No. 186 at 3.
6 It seems highly unlikely that this was the type of information the Supreme Court intended to
7 protect with the *Reynolds* privilege.

8 Furthermore, the Government’s voluntary reliance on the Classified Declaration for more
9 than two years in litigating this case (*see* Dkt. No. 144) contradicts the Government’s current
10 claim that the same evidence is too sensitive to be used in litigation. The Government’s delay in
11 invoking the state secrets privilege until Twitter’s cleared counsel has requested access suggests
12 that the privilege claim has little to do with the sensitivity of the information and everything to
13 do with litigation tactics.

14 The Government tries to avoid this inference by characterizing its belated assertion of the
15 privilege as demonstrating “restraint.” *See* Dkt. No. 281 at 21–22. But given that the
16 Government is attempting to use the privilege to force the Court to deny Twitter access to the
17 Classified Declaration, *see infra*, pp. 11–12, this case is no study in Executive restraint.

18 Indeed, even if the Court *agreed* that disclosure to cleared counsel posed too great a risk
19 of inadvertent disclosure, that would warrant only denying Twitter’s access request under the
20 Court’s broad authority to control discovery as necessary “to balance [the] need for access to
21 proof ... against the extraordinary needs of the [Executive agencies] for confidentiality.”
22 *Webster*, 486 U.S. at 604. It would not provide a valid basis to uphold the Government’s
23 privilege claim and remove the Classified Declaration from evidence.

24 The “long lapse of time” since the events addressed in the Classified Declaration
25 provides yet another reason to doubt the merits of the Government’s state secrets claim. *See In*
26 *re U.S.*, 872 F.2d at 479. If the Classified Declaration—which was filed with the Court in
27 December 2016 and seeks to justify the suppression of information from 2013—was not too
28 sensitive to be used in this litigation two years ago, it is hard to see how its apparently “generic”

1 and “boilerplate” contents have become *more* sensitive with time. Dkt. No. 172, at 18. The
 2 Court should consider the sensitivity of the information in light of the circumstances as they exist
 3 *now*, when further disclosure is actually being contemplated, and “not when the affidavit was
 4 prepared or the material filed with the court.” *United States v. Ahmad*, 499 F.2d 851, 855 (3d
 5 Cir. 1974). Even the Government’s own regulations recognize that the passage of almost three
 6 years can profoundly affect the ongoing need for secrecy. Nondisclosure obligations for NSLs
 7 presumptively “terminate when the underlying investigation is closed” or “on the three-year
 8 anniversary of the initiation of the investigation.”²

9 Finally, the Government contends that any information in the Classified Declaration
 10 about Twitter’s receipt of national security process (much of which presumably pertains to
 11 aggregate reporting from five years ago) is a “state secret”—and thus must be excluded from
 12 evidence in this litigation. That position cannot be squared with the Court’s determination that
 13 the Classified Declaration did not show that even *public* disclosure of materially identical
 14 information in Twitter’s 2014 draft Transparency Report would cause sufficient harm to national
 15 security to justify restrictions on public reporting of it. And a fully unredacted version of
 16 Twitter’s 2014 draft Transparency Report is in evidence under seal (*see* Dkt. No. 21-1
 17 (November 17, 2014)), with no claim of resulting harm to national security. Additionally, that
 18 information is already known to Twitter agents without a security clearance (and thus subject to
 19 the same risk of inadvertent disclosure that the Government claims is intolerable in this
 20 litigation), without any resulting harm to national security. *See, e.g.*, 50 U.S.C. § 1861(d)(1)(A)–
 21 (B) (authorizing disclosure of the fact of FISA process to persons, including attorneys, necessary
 22 for compliance).

23 Yet the Government now—for the first time—suggests that the state secrets privilege
 24 applies to an acknowledgement by Twitter that it was served with NSL or FISA process even
 25 once over the past several years. That information cannot possibly qualify as a state secret
 26

27 ² *In re NSL*, 863 F.3d at 1118 (discussing Termination Procedures for National Security Letter
 28 Nondisclosure Requirement, Fed. Bureau of Investigation (Nov. 24, 2015),
<https://www.fbi.gov/file-repository/nsi-ndp-procedures.pdf>).

1 because it is already effectively in the public domain. *See Hepting v. AT&T Corp.*, 439 F. Supp.
 2 2d 974, 990–91, 995 (N.D. Cal. 2006). It is already public knowledge, for example, that many of
 3 Twitter’s peers, including Yahoo, Google, and Microsoft, have received FISA orders and
 4 mounted a challenge to associated non-disclosure obligations in the FISC. Likewise, the
 5 Government has made publicly available a petition (initially classified as Top Secret) by Yahoo
 6 challenging certain aspects of the FISA which contains far more detail about Yahoo’s receipt of
 7 FISA process than the aggregate figures at issue here, *see*
 8 <https://fas.org/irp/agency/doj/fisa/fiscr082208-2014.pdf>.

9 Moreover, numerous other suits over nondisclosure obligations relating to national
 10 security process have been litigated without evident harm to national security. *See, e.g., In re*
 11 *NSL*, 863 F.3d at 1119–20; *Doe, Inc. v. Mukasey*, 549 F.3d 861, 864 (2d Cir. 2008); *Doe v.*
 12 *Gonzales*, 386 F. Supp. 2d. 66 (D. Conn. 2005). One case publicly disclosed the names of the
 13 recipients challenging nondisclosure orders (CloudFlare and CREDO)—including a
 14 nondisclosure order that “remain[ed] in full effect.” *In re NSL*, 863 F.3d at 1120. In fact, the
 15 FBI’s apparent basis for determining that CloudFlare’s identity “may be publicly identified” was
 16 that CloudFlare was “challenging two NSLs.” *Id.* at 1120 n.15. If the fact of receipt was not a
 17 state secret in that case, then it cannot be a state secret as to Twitter—a platform with millions of
 18 users that has already lawfully disclosed to the public that it receives national security process.
 19 In addition to the aggregate reports it issues in accordance with the USA Freedom Act bands,
 20 Twitter has in recent years published 14 NSLs, revealing not only the fact of receipt but also the
 21 precise date each NSL was received. Declaration of Linda Isley (“Isley Decl.”), ¶¶ 3–6, Ex. A–
 22 C. This information precludes any potential adversary from thinking that Twitter is not a
 23 recipient of national security process, *see* Dkt. No. 281, at 14, and the Government has pointed to
 24 no other information adversaries could possibly glean were they to learn that Twitter also
 25 (hypothetically) received process under the FISA.³

26
 27 ³ These disclosures were possible only because of the recently strengthened judicial review
 28 procedures in the NSL statute. The fact that—now subject to judicial scrutiny—the Government
 repeatedly has failed to justify any ongoing need for nondisclosure of NSLs underscores the
 importance of Twitter’s challenge to the absence of any comparable judicial review provisions

1 In sum, the public record provides numerous, independent reasons to doubt that
 2 continued use of the Classified Declaration, under seal and *in camera*, would pose such an
 3 intolerable risk to national security as to require its exclusion from evidence.

4 **3. The Ninth Circuit has repeatedly held that mere classification does not**
 5 **render information a state secret.**

6 The Government’s proffered justifications for its privilege claim are facially deficient.
 7 Much of the Government’s briefing and declarations focus on the harm that it claims would flow
 8 from disclosure of the information in the Classified Declaration to “*adversaries of the United*
 9 *States*”—not to cleared counsel. *See* Dkt. No. 281, at 14 (emphasis added). But Twitter is not
 10 seeking to publicly disclose the Classified Declaration.

11 Showing that disclosure of the Classified Declaration to adversaries would harm national
 12 security would establish only that the specified information is properly classified. *See* Executive
 13 Order (“EO”) 13526, § 1.2(a)(3) (the “confidential” classification applies “to information, the
 14 unauthorized disclosure of which reasonably *could be expected to cause damage to the national*
 15 *security*.” (emphasis added)); *see also id.* § 1.2(a)(2) (the “secret” classification applies to
 16 information that would result in “serious” harm to national security).

17 But the Ninth Circuit has repeatedly explained that “not all classified information is
 18 necessarily privileged under *Reynolds*.” *Fazaga*, 916 F.3d at 1227; *Jeppesen*, 614 F.3d at 1082.
 19 Classification focuses on the national security risk associated with disclosure of information to
 20 persons who have *not* been deemed suitable to view classified information. *See* EO 13526; *see*
 21 *generally* Dkt. Nos. 145, 145-1 (arguing that Twitter’s draft Transparency Report is properly
 22 *classified* because its unauthorized disclosure would provide foreign “adversaries” with
 23 information that could harm national security). Similarly, the Freedom of Information Act
 24 (“FOIA”), obligates an agency to “make available to the public” certain categories of
 25 information if it cannot justify them as “properly classified” under FOIA Exemption 1. *See* 5

26 _____
 27 for aggregate reporting restrictions in the FISA regime. *See* Dkt. No. 183 (Twitter Opposition to
 28 Motion for Reconsideration), at 3–4, 14–16. It would be Kafkaesque, to say the least, to find
 judicial review precluded where the very thrust of Twitter’s claims is that the unavailability of
 judicial review is what makes the FISA regime unconstitutional.

1 U.S.C. §§ 552(a), (b)(1) (assuming, of course, that no other exemption applies).

2 In contrast, the state secrets privilege properly focuses on the risk associated with use of
 3 classified evidence under seal to a very limited subset of persons who have been deemed suitable
 4 to view the classified information—persons whose access to the classified information, by
 5 definition, does not pose a risk of harm to national security. And if a state secrets privilege claim
 6 over classified evidence is denied, the result is not public disclosure, but rather use of the
 7 evidence under appropriate safeguards. Thus, when the Government seeks removal of classified
 8 information from evidence under the state secrets privilege, it must demonstrate that the evidence
 9 is too sensitive to be used in litigation at all under any conceivable procedural safeguards. The
 10 Government cannot make that heightened showing here. It offers no reasonable basis to fear that
 11 disclosure of the Classified Declaration to cleared counsel will pose a serious threat to national
 12 security.

13 **4. The Government relies on categorical—and insupportable—assumptions**
 14 **regarding the risk of national security harm associated with granting**
Twitter’s cleared counsel access to the Classified Declaration.

15 The Government concedes that its sole reason for invoking the state secrets privilege
 16 over the Classified Declaration “now” is “the continued pendency of the Plaintiff’s request for
 17 access to the Classified Steinbach Declaration, and the Order to Show Cause why it should not
 18 be disclosed.” Dkt. No. 281, at 22. Indeed, the Government asserts that denying Twitter’s
 19 request for access would eliminate the basis for a state secret designation. *See id.* at 11–12
 20 (inviting the Court to “avoid[] the need to reach the state secrets privilege assertion” by
 21 “discharg[ing] the Order to show cause on other grounds”); *id.* at 21 (The Government “has not
 22 invoked the state secrets privilege until it became necessary to do so to protect against a potential
 23 order of disclosure.”).

24 The Government’s conditioning of its privilege assertion on the risk that the Court might
 25 order disclosure of the Classified Declaration to Twitter’s cleared counsel reveals that it is using
 26 the state secrets privilege as a tactical weapon, rather than out of genuine concern about the
 27 sensitivity of the Classified Declaration. And this litigation-driven position could lead to an
 28

1 anomalous result: Upholding the Government’s invocation of the state secrets privilege here
 2 does not simply prevent the disclosure of the Classified Declaration to private cleared counsel—
 3 the Government’s only asserted concern—but altogether removes the Classified Declaration
 4 from evidence. This misalignment between the risk claimed to justify the Government’s state
 5 secrets assertion and the consequence of upholding it illustrates why the assertion is
 6 inappropriate here. Indeed, dismissal of the case would effectively penalize Twitter for seeking
 7 access to the Classified Declaration. That perverse result underscores that the state secrets
 8 privilege is not the appropriate mechanism to protect the Government’s claimed national security
 9 concerns.

10 Indeed, like its need-to-know objection, the Government’s state secrets claim appears to
 11 be just another attempt to supplant the Court’s gatekeeping role in discovery. *See* Dkt. No. 281,
 12 at 22–23. But that by-hook-or-by-crook approach flies in the face of the separation-of-powers
 13 principles discussed in Twitter’s Opposition to the Government’s Response to Order to Show
 14 Cause, Dkt. No. 265 (at 5–12); *see also e.g., Unigard Sec. Ins. Co. v. Lakewood Eng’g & Mfg.*
 15 *Corp.*, 982 F.2d 363, 368 (9th Cir. 1992); *Horn v. Huddle*, 647 F. Supp. 2d 55, 65 & n.18
 16 (D.D.C. 2009), *vacated due to settlement as discussed in Horn v. Huddle*, 699 F. Supp. 2d. 236,
 17 237–38 (D.D.C. 2010) (*see* Twitter’s discussion at Dkt. No. 265, at 9 n.5); *In re Nat’l Sec.*
 18 *Agency Telecomms. Records Litig.*, 595 F. Supp. 2d 1077, 1089 (N.D. Cal. 2009).

19 The assumptions underlying the Government’s privilege claim are insupportable. The
 20 Government emphasizes that its invocation of state secrets has nothing to do with any
 21 “individualized findings as to the trustworthiness of Plaintiff’s counsel,” but is based on a
 22 categorical view that *any* use of classified information by “cleared private counsel for non-
 23 governmental parties in civil litigation” presents an “unjustifiable,” incremental risk of
 24 unauthorized disclosure. Dkt. No. 281, at 19; Dkt. No. 281-2, ¶ 38. That position fails for at
 25 least three reasons.

26 **First**, if accepted, the same argument would apply to *any* classified information, which
 27 runs afoul of the Ninth Circuit’s admonition that the mere fact of classification does not make
 28 evidence a state secret. *See Fazaga*, 916 F.3d at 1227.

1 **Second**, the Government’s premise—that “every additional disclosure” of classified
 2 information to private counsel in a civil case invariably poses “an unjustifiable risk of harm to
 3 national security” (Dkt. No. 281, at 18–19)—is demonstrably wrong. The Government muses
 4 that private civil attorneys cannot abide by safeguards necessary to protect the secrecy of
 5 classified information, because they have obligations to advocate for their clients. *See* Dkt. No.
 6 281, at 19. But private counsel in criminal cases have the same obligation, and the Criminal
 7 Information Procedures Act (“CIPA”) specifically contemplates the use of classified evidence in
 8 criminal litigation, *see* 18 U.S.C. App. 3 § 6(a), (f) (recognizing that district court may decide
 9 whether “classified information may be disclosed in connection with a trial or pretrial
 10 proceeding”), *id.* § 7(a) (authorizing interlocutory appeal from court order “imposing sanctions
 11 for nondisclosure of classified information”); *id.* § 8 (setting forth procedures for the
 12 “[i]ntroduction of classified information” into evidence).

13 Nor are civil litigators necessarily “less familiar[] with the necessary safeguards to
 14 protect classified information” than government attorneys. Dkt. No. 281, at 19. Many private
 15 counsel (including Twitter’s counsel here) have experience safely handling classified material—
 16 including by virtue of prior representations in criminal matters that required access to and review
 17 of classified material.⁴ *See* Rubin Decl. ¶¶ 2–4. Moreover, as CIPA illustrates, courts have a
 18 variety of tools to guard against unnecessary disclosure of classified information—including
 19 redaction of the most sensitive classified information, 18 U.S.C. App. 3, § 4, *in camera*
 20 proceedings, and the sealing of court records (including court orders) to the extent necessary to
 21 protect the secrecy of classified information, *id.* § 6(a), (d); *see also In re Sealed Case*, 494 F.3d
 22 at 154 (suggesting that CIPA’s procedural safeguards could likewise be applied to protect
 23 classified evidence in civil proceedings so that a plaintiff’s claims “could proceed”).

24 Contrary to the Government’s contention, courts have repeatedly entrusted private civil

25

 26 ⁴ Moreover, Twitter’s counsel has already recognized that any notes or briefs related to the
 27 classified material would need to be prepared on secure computers located in a Sensitive
 28 Compartmented Information Facility (“SCIF”), *see* Rubin Decl., ¶ Ex. 5 (11.26.2018 Hr. Tr. at
 10:15–11:11), belying the Government’s professed concern about “privileged notes and work
 product on computers to which the Government would have no access,” Dkt. No. 281, at 19; *see*
also id. at 20.

1 counsel with access to classified information central to the litigation. In *Loral Corporation v.*
 2 *McDonnell Douglas Corp.*, for example, the Second Circuit permitted a trial to proceed in a
 3 contract case even though “a large amount of material properly classified confidential and secret
 4 must be submitted to the trier of fact.” 558 F.2d 1130, 1132 (2d Cir. 1977). While
 5 acknowledging that a “jury trial is not a practicable possibility” in these circumstances, the court
 6 observed that “[t]he Department of Defense has cleared, or can and will clear, for access to the
 7 material the judge and magistrate assigned to the case, *the lawyers* and any supporting personnel
 8 whose access to the material is necessary.” *Id.* (emphasis added). *Halpern v. United States*
 9 likewise remanded a civil patent claim back to the district court for trial *in camera*—over the
 10 Government’s assertion that the state secrets privilege required outright dismissal of the
 11 Plaintiff’s claims. *See* 258 F.2d 36, 44 (2d Cir. 1958).

12 These precedents accord with *Webster v. Doe*, another civil case. In *Webster*, the
 13 Supreme Court observed that “the District Court has latitude to control any discovery process
 14 which may be instituted so as to balance respondent’s need for access to proof which would
 15 support a colorable constitutional claim against the extraordinary needs of the [government] for
 16 confidentiality and the protection of its methods, sources, and mission.” 486 U.S. at 604.

17 ***Third***, the Government provides no authority for its view that disclosure of classified
 18 evidence to cleared counsel in civil matters invariably poses an unreasonable risk of harm to
 19 national security. In fact, the Ninth Circuit has stated precisely the opposite: “[A] lawyer for the
 20 designated entity who has the appropriate security clearance ... does not implicate national
 21 security when viewing the classified material because, by definition, he or she has the
 22 appropriate security clearance.” *Al Haramain II*, 686 F.3d at 983. Thus, “[i]n many cases, ...
 23 some information could be summarized or *presented to a lawyer with a security clearance*
 24 *without implicating national security*.” *Id.* (emphases added).

25 To be sure, *Al Haramain II* declined categorically to hold that cleared counsel may
 26 *always* access relevant classified information, noting that, “[d]epending on the circumstances,
 27 [the government] might have a legitimate interest in shielding [classified] materials even from
 28 someone with the appropriate security clearance.” *Id.* (emphasis added). The Ninth Circuit

1 suggested, for example, that a particular “surveillance operation” might be so sensitive that the
 2 Attorney General could have “a legitimate interest” in preventing its disclosure to anyone “not
 3 involved in the surveillance.” *Id.* (quoting *United States v. Ott*, 827 F.2d 473, 477 (9th Cir.
 4 1987)); *but compare Kinoy v. Mitchell*, 67 F.R.D. 1, 13 (S.D.N.Y. 1975) (rejecting “conclusory”
 5 state secrets claim in wiretapping case absent showing that material consisted of “confidential
 6 deliberations or informers’ identities”). But governing law’s consistent reliance on a case-by-
 7 case approach contradicts the Government’s categorical assumption that any access to classified
 8 evidence by cleared counsel in civil litigation automatically “create[s] an unjustifiable risk of
 9 harm to national security.” Dkt. No. 281, at 19.

10 The Government’s other authorities (*see* Dkt. No. 281, p. 19 & n.4) are even further
 11 afield. *Jeppesen, El-Masri, Sterling*, and *Halkin* merely recognize the undisputed proposition
 12 that, where the state secrets privilege has been *properly* invoked, neither the plaintiff nor his
 13 cleared counsel may access the evidence. *See El-Masri v. United States*, 479 F.3d 296, 312 (4th
 14 Cir. 2007); *accord Sterling v. Tenet*, 416 F.3d 338, 345–46 (4th Cir. 2005); *Halkin*, 598 F.2d at
 15 7. And *Ellsberg* merely recognized that “*the legitimacy of a state secrets privilege claim*
 16 *should,*” like all privilege claims, be determined based on *in camera, ex parte* proceedings. 709
 17 F.2d 51, 61 (D.C. Cir. 1983) (emphasis added).

18 Twitter is not seeking to participate in any *in camera* proceedings relating to the
 19 Government’s *privilege* claim, however, such as the Court’s review of the Classified McGarrity
 20 Declaration. Rather, Twitter contends that the Classified *Steinbach* Declaration is *not*, in fact, a
 21 state secret, and that its cleared counsel should therefore be entitled to see that evidence, as
 22 necessary to participate in any *in camera, merits* proceedings.

23 Finally, the Ninth Circuit in *Fazaga* rejected precisely the kind of categorical bar to
 24 access to classified evidence in civil proceedings that the Government invokes here. There, the
 25 court confirmed that the procedural rules authorizing courts to disclose classified information to
 26 litigants challenging the lawfulness of Government surveillance “*apply in both civil and criminal*
 27 *cases, and to both affirmative and defensive use of electronic surveillance evidence.*” 916 F.3d at
 28 1237 (emphasis added) (citing H.R. Rep. No. 95-1720, at 32).

1 Nor is there any merit to the Government’s concern that granting Twitter’s cleared
 2 counsel access to discrete, highly relevant evidence would “vastly extend” private litigants’
 3 ability to access classified information on “topics of their choice[] simply by bringing lawsuits
 4 that put such information at issue.” Dkt. No. 281, at 19. As both Section 1806(f) and *Al-*
 5 *Haramain II* illustrate, the *status quo* has been case-by-case assessment of cleared counsel’s need
 6 for access to classified materials; that approach has not produced unfettered public access to
 7 classified information.⁵ This is not a FOIA case seeking access to classified information for the
 8 purpose of *public* disclosure (rather than for purposes of resolving constitutional claims). And
 9 this case has equally little in common with a government employee case, where the employee
 10 has voluntarily relinquished certain First Amendment rights in exchange for employment. *See*
 11 Dkt. No. 172, at 19. The invocation of the state secrets privilege cannot hinge on a one-size-fits-
 12 all claim that any private counsel’s access to classified evidence in a civil case raises an
 13 intolerable risk of harm to national security.

14 In sum, the Government’s categorical position is at odds with governing precedent,
 15 Congressional intent, and practical experience. And the Government has disclaimed that its
 16 privilege claim is based on any kind of “individualized” assessment of the risk of harm to
 17 national security from the continued use of the Classified Declaration in this litigation subject to
 18 the protective tools available to the Court. Dkt. No. 281, at 19.

19 Because the privilege “by [its] very nature hinder[s] the ascertainment of the truth, and
 20 may even torpedo it entirely,” it must be “limited” to those cases in which it is necessary to
 21 achieve its “narrowest purpose.” *In re U.S.*, 872 F.2d at 478–79 (denying mandamus petition
 22 seeking state secrets protection). Accordingly, even if the Court agrees that disclosure to
 23 Twitter’s cleared counsel would pose a national security risk, the Court could negate that risk by
 24 denying Twitter’s request for access under its broad discovery powers and maintaining the
 25 Classified Declaration *ex parte*. The availability of this alternative further underscores that the
 26

27 ⁵ *Cf. Am.-Arab Anti-Discrimination Comm. v. Reno*, 70 F.3d 1045, 1071 (9th Cir. 1995)
 28 (affirming, long before *Al-Haramain II*, that the government could not use “undisclosed
 classified information in legalization proceedings”).

1 state secrets privilege is far too blunt an instrument to accommodate the Government’s claimed
 2 national security interests, and its invocation runs afoul of the rule that a privilege assertion
 3 should be upheld only where necessary to serve its “narrowest purpose.”

4 **B. Dismissal Is Not Warranted Even if Some Portions of the Classified Declaration**
 5 **Qualify as State Secrets.**

6 Even if the Court finds that some portion of the Classified Declaration has been properly
 7 designated a state secret, that would not permit dismissal of Twitter’s claims for two independent
 8 reasons. First, the NSL and FISA statutes reflect a clear Congressional intent to ensure a forum
 9 for judicial review of challenges to nondisclosure obligations imposed in connection with the
 10 Executive’s electronic surveillance activities. *See Fazaga*, 916 F.3d at 1226. And second,
 11 removal of the Classified Declaration from this case would warrant dismissal only if the
 12 Classified Declaration provided a “valid defense” to Twitter’s constitutional claims. *Id.* at 1253.
 13 The Court has already determined that it does not. *See* Dkt. Nos. 172, 186.

14 **1. The FISA and NSL statutes reflect a Congressional intent to provide a**
 15 **judicial forum for challenges to restrictions on aggregate disclosure of**
 16 **national security process.**

17 The Government’s motion to dismiss Twitter’s claims—indeed, even its invocation of
 18 state secrets more broadly—is fundamentally at odds with Congress’s clear intent in enacting the
 19 FISA and NSL regimes to ensure judicial review of nondisclosure obligations imposed on
 20 recipients of national security process.

21 The Ninth Circuit recently recognized a similar intent in *Fazaga*, where it found that
 22 Congress had preempted the state secrets privilege as to targets of FISA surveillance. 916 F.3d
 23 at 1238. In so holding, the court observed that “[t]he state secrets privilege is a[] ... federal
 24 common law” “evidentiary privilege.” *Id.* at 1230 (quoting *Al-Haramain I*, 507 F.3d at 1196);
 25 *see also Gen. Dynamics Corp. v. United States*, 563 U.S. 478, 485 (2011) (“*Reynolds* decided
 26 a purely evidentiary dispute by applying evidentiary rules.”). It may therefore be “displaced” by
 27 any Congressional act which “speak[s] directly to the question” ““otherwise answered by federal
 28 common law.”” *Id.* at 1231 (quoting *Kasza v. Browner*, 133 F.3d 1159, 1167 (9th Cir. 1998)).
 The Court held that Congress had so spoken in 50 U.S.C. § 1806(f)—the provision of FISA

1 which authorizes and governs discovery in suits by targets of electronic surveillance. The Court
 2 reasoned that Section 1806(f) reflected a Congressional intent to “override[] ... the state secrets
 3 evidentiary dismissal option” in favor of a “mandatory,” “alternative mechanism for
 4 consideration of electronic state secrets evidence.” *Id.*, 916 F.3d at 1231–32. The court inferred
 5 this legislative intent from the facts that (1) “[t]he procedures set out in § 1806(f) are animated
 6 by the same concerns—threats to national security—that underlie the state secrets privilege,” *id.*;
 7 (2) FISA “includes a private civil enforcement mechanism, and sets out a procedure by which
 8 courts should consider evidence that could harm the country’s national security,” *id.* (citing 50
 9 U.S.C. §§ 1806(f), 1810); and (3) “FISA was enacted in response to ‘revelations that warrantless
 10 electronic surveillance in the name of national security ha[d] been seriously abused,’” *id.* at 1233
 11 (quoting S. Rep. No. 95-604, pt. 1, at 7 (1978), reprinted in 1978 U.S.C.C.A.N. 3904, 3908).

12 Though Section 1806(f) does not govern the precise claims brought here, other provisions
 13 of the NSL and FISA schemes demonstrate the same Congressional intent to ensure a forum for
 14 judicial review for challenges to non-disclosure obligations by statute or court order.

15 Title V of FISA, for example, sets forth detailed procedures for “[j]udicial review” of
 16 FISA “nondisclosure order[s]” accompanying FISA applications for business records. 50 U.S.C.
 17 § 1861(f)(2)(A)(i) (“A person receiving a production order may challenge the legality of ... *any*
 18 *nondisclosure order imposed in connection with the production order* by filing a petition with
 19 the” FISA court “established by section 1803(e)(1)” (emphasis added)); *cf. id.* § 1861(f)(4)–(5)
 20 (setting forth procedures to accommodate national security concerns, including sealing of court
 21 records, and the availability of *ex parte* and *in camera* review).

22 Likewise, the judicial review provision in the NSL statute, 18 U.S.C. § 3511, includes
 23 nearly all the attributes that led the Court in *Fazaga* to find the state secrets dismissal remedy
 24 preempted. For example, section 3511(a) “includes a private civil enforcement mechanism,”
 25 *Fazaga*, 916 F.3d at 1232, whereby a “recipient of a request for records” may “petition” any
 26 district court “for an order modifying or setting aside the request,” 18 U.S.C. § 3511(a). And,
 27 like review under FISA, Section 3511(a) review is “triggered by a process—the filing of an
 28 affidavit under oath by the Attorney General—nearly identical to the process that triggers

1 application of the state secrets privilege,” *Fazaga*, 916 F.3d at 1232; *see* 18 U.S.C. § 3511(b)(2)
2 (requiring “certification from [an agency head] ... containing a statement of specific facts
3 indicating that the absence of a prohibition of disclosure under this subsection may result in
4 [harm to national security].”). Subdivisions (d) and (e) likewise set out the procedural
5 safeguards to be used in these civil proceedings to protect classified evidence, including
6 “close[d] ... hearing[s],” *id.* § 3511(d); sealing of any court records “to the extent and as long as
7 necessary to prevent the[ir] unauthorized disclosure,” *id.*; and “ex parte and in camera” review,
8 *id.* § 3511(e). Moreover, a driving force behind the NSL review provisions was the “serious
9 misuse and abuse of national security letters” documented in audits by the “Justice Department’s
10 Inspector General.” Senate Committee on the Judiciary, National Security Letters: The Need for
11 Greater Accountability and Oversight, Serial No. J-110-86 (April 23, 2008) (Sen. Feingold).

12 Neither of these provisions relates directly to aggregate reporting—indeed, the absence of
13 a clear avenue for expeditious, judicial review of restrictions on aggregate reporting is a principal
14 defect that Twitter has challenged in this case as unconstitutional. But the Government has taken
15 the position in this litigation that restrictions on aggregate reporting stem from the collective
16 nondisclosure orders included in each individual NSL and FISA information request. *See, e.g.*,
17 Rubin Decl. ¶ 6, Ex. B (Defendants’ Responses to Interrogatories, Set Two, No. 6); Dkt. No.
18 290, at 2–3. And if that is so, then it would frustrate Congress’s manifest intent to preclude the
19 invocation of the state secrets privilege in proceedings challenging the legality of individual
20 nondisclosure requirements, but to permit invocation of the privilege—and the possibility of
21 dismissal as a remedy—in challenges to restrictions on aggregate reporting. Indeed, allowing the
22 Government to evade judicial review under the cover of state secrets makes even less sense in
23 the aggregate reporting setting, where challenges are far more likely to focus on more general
24 questions about the recipient of national security process (rather than case-specific details about
25 individual targets of surveillance).

26 In sum, Congress’s intent here is clear: Twitter’s claims should be permitted to proceed,
27 subject to any procedural safeguards the Court may deem appropriate.
28

1 **2. Dismissal also is not warranted here because a finding of state secrets would**
 2 **not deprive Defendants of a *valid* defense.**

3 Independently, dismissal is not warranted here because even wholesale exclusion of the
 4 Classified Declaration would not deprive the Government of a “valid defense” to Twitter’s
 5 claims. To qualify as “valid,” the Government’s defense must be *more* than merely “plausible or
 6 colorable.” *Fazaga*, 916 F.3d at 1253 (quoting *In re Sealed Case*, 494 F.3d at 150). Rather, a
 7 “valid defense” is one that “is meritorious ... and would require judgment for the defendant.” *Id.*
 8 (quotation marks omitted).⁶ This rule makes perfect sense. If it were otherwise, the Government
 9 could obtain dismissal of a case simply by claiming that all manner of sensitive military secrets
 10 were essential to its case, regardless of whether the information actually constituted a
 11 “meritorious” defense. *See id.*

12 The Government plainly cannot show that the Classified Declaration provides a “valid
 13 defense” as the Court has already twice rejected it as insufficient to rebut Twitter’s claim that the
 14 restrictions on Twitter’s speech in the 2014 draft Transparency Report (and like reports) are
 15 unconstitutional. *See* Dkt. Nos. 172, 186.

16 **3. Ample mitigation measures are available here to protect any state secrets.**

17 The Government also overlooks the Ninth Circuit’s instruction that dismissal should be
 18 reserved for “rare” cases. *Am.-Arab Anti-Discrimination Comm.*, 70 F.3d at 1070. “Ordinarily,”
 19 the Ninth Circuit has observed, “simply excluding or otherwise walling off the privileged
 20 information may suffice to protect the state secrets and ‘the case will proceed accordingly, with
 21 no consequences save those resulting from the loss of evidence.’” *Jeppesen*, 614 F.3d at 1082
 22 (quoting *Al-Haramain I*, 507 F.3d at 1204); *accord Fazaga*, 916 F.3d at 1227 (“Because there is
 23 a strong interest in allowing otherwise meritorious litigation to go forward, the court’s inquiry
 24 into the need for the secret information should be specific and tailored, not vague and general.”).

25

 26 ⁶ Were the rule otherwise, the Ninth Circuit has recognized, “virtually every case in which the
 27 United States successfully invokes the state secrets privilege would need to be dismissed.”
 28 *Fazaga*, 916 F.3d at 1253. Yet that “would constitute judicial abdication from the responsibility
 to decide cases on the basis of evidence,” as well as “run afoul” of the Supreme Court’s
 “caution[] against” overbroad interpretation of evidentiary privileges that “preclud[e] review of
 constitutional claims.” *Id.* (citing *In re Sealed Case*, 494 F.3d at 151).

Accordingly, “[w]henver possible, sensitive information must be disentangled from nonsensitive information to allow for the release of the latter.” *Jeppesen*, 614 F.3d at 1082 (quoting *Kasza*, 133 F.3d at 1166). For example, if an informant’s name could be “redacted” without losing the substance of the Government’s argument, the mere fact that the name might qualify as a state secret would not require dismissal. *See In re U.S.*, 872 F.2d at 477. This approach seems particularly suited to protecting any information in the Government’s fourth category of its alleged state secrets privilege assertion—“[i]nformation revealing specific targets of investigation and activities of adversaries of the United States.” Dkt. No. 281-1, ¶¶ 4(iv), 11. Though the Court’s description of the Classified Declaration in its prior orders gives Twitter reason to doubt that any information in this category is sufficiently specific or timely to qualify as a “state secret,” to the extent such details do exist, they almost certainly are not essential to the Government’s reasons for claiming that aggregate reporting more granular than the USA Freedom Act bands would harm national security. Likewise, the fact that the relevance of the alleged state secrets is largely confined to the Government’s defense weighs strongly against dismissal, because “[t]he Government retains a large measure of control and judgment over its own evidence,” which greatly “reduces the possibility of unauthorized disclosure of confidential material.” *In re U.S.*, 872 F.2d at 478; *see also In re Sealed Case*, 494 F.3d at 154 (observing that even “[i]n *Reynolds* itself, [decided] at the height of the Cold War, the Supreme Court remanded the FTCA case to proceed without the privileged materials”).

CONCLUSION

The Court should (1) deny the Government’s assertion of state secrets over the Classified Declaration; (2) deny the Government’s motion to dismiss Twitter’s claims; and (3) grant Twitter’s request that its cleared counsel be granted access to the Classified Declaration under procedural safeguards that the Court deems appropriate.

1 Dated: April 29, 2019

MAYER BROWN LLP

2 /s/ Lee H. Rubin

3 LEE H. RUBIN (SBN 141331)

4 lrubin@mayerbrown.com

DONALD M. FALK (SBN 150256)

5 dfalk@mayerbrown.com

SAMANTHA C. BOOTH (SBN 298852)

sbooth@mayerbrown.com

6 Two Palo Alto Square, Suite 300

3000 El Camino Real

7 Palo Alto, CA 94306-2112

Telephone: (650) 331-2000

8 Facsimile: (650) 331-2060

9 Attorneys for Plaintiff

10 TWITTER, INC.

1 MAYER BROWN LLP
ANDREW JOHN PINCUS (*Pro Hac Vice*)
2 apincus@mayerbrown.com
1999 K Street, NW
3 Washington, DC 20006
Tel: (202) 263-3220 / Fax: (202) 263-3300
4

MAYER BROWN LLP
5 LEE H. RUBIN (SBN 141331)
lrubin@mayerbrown.com
6 DONALD M. FALK (SBN 150256)
dfalk@mayerbrown.com
7 SAMANTHA C. BOOTH (SBN 298852)
sbooth@mayerbrown.com
8 Two Palo Alto Square, Suite 300
3000 El Camino Real
9 Palo Alto, CA 94306-2112
Tel: (650) 331-2000 / Fax: (650) 331-2060
10

Attorneys for Plaintiff Twitter, Inc.
11

12 **UNITED STATES DISTRICT COURT**
13 **NORTHERN DISTRICT OF CALIFORNIA**
14 **OAKLAND DIVISION**

15 TWITTER, INC.,

16 Plaintiff,

17 v.

18 WILLIAM P. BARR, Attorney General of the
19 United States, *et al.*,

20 Defendants.
21

Case No. 14-cv-4480-YGR

**DECLARATION OF LEE H. RUBIN IN
SUPPORT OF TWITTER, INC.'S
OPPOSITION TO DEFENDANTS'
INVOCATION OF STATE SECRETS
AND MOTION TO DISMISS**

1 I, Lee H. Rubin declare as follows:

2 1. I am a partner in the law firm of Mayer Brown LLP and lead counsel to Plaintiff
3 Twitter, Inc. (“Twitter”), in the above-captioned action. I submit this declaration in support of
4 Twitter’s Opposition to Defendants’ Invocation of State Secrets and Motion to Dismiss. Unless
5 otherwise indicated, this declaration is based on my personal knowledge, and if called as a
6 witness, I could and would testify competently to the matters discussed herein.

7 2. Since leaving the Department of Justice in September 1997 and practicing as a
8 private lawyer at Mayer Brown LLP, I have been involved in two previous matters that required
9 me to submit to an FBI background investigation and obtain a security clearance in order to have
10 access to classified information to represent my clients.

11 3. In 1998, I served as counsel for Theresa Squillacote in *United States v.*
12 *Squillacote*, CR 98-61 (E.D. Va), in the Government’s prosecution of Ms. Squillacote and her
13 husband for various espionage-related offenses. Because the defense of Ms. Squillacote required
14 review of classified information, I submitted to an FBI background investigation and, at the
15 conclusion of that investigation, was favorably adjudicated to receive a security clearance.
16 I was subsequently granted a security clearance. In the course of my representation of Ms.
17 Squillacote, I reviewed scores of classified documents within a Sensitive Compartmented
18 Information Facility (“SCIF”) and prepared classified submissions on a secure computer within a
19 Government SCIF. I also participated in a closed hearing pursuant to the Classified Information
20 Procedures Act that included classified testimony.

21 4. In 2007, I was retained to serve as counsel for a defense/security contractor in
22 connection with an investigation of the company conducted by the Department of Justice. In
23 order to represent the company, I was required to review classified information. Accordingly, I
24 submitted to an FBI background investigation and, at the conclusion of that investigation, was
25 favorably adjudicated to receive a security clearance. I was subsequently granted a security
26 clearance. In the course of my representation of the company, I reviewed classified material and
27 interviewed company witnesses in a SCIF regarding classified information related to the
28

1 Government's investigation. I also attended Government interviews of company witnesses that
2 involved the discussion of classified information and prepared submissions to the Government
3 that included classified information. The latter activities also took place within a SCIF.

4 5. As counsel to Twitter in this litigation, I have committed to abiding by whatever
5 procedural safeguards the Court may deem appropriate to protect classified information.

6 Attached hereto as **Exhibit A** is a true and correct copy of an excerpt from the November 26,
7 2018 hearing before this Court reflecting that commitment.

8 6. On or about March 13, 2018, Defendants served responses to Twitter's Second
9 Set of Interrogatories. Interrogatory No. 6 asked Defendants to "[i]dentify the operative
10 provision(s) of any statute, regulation, policy, procedure, order, or other authority which You
11 contend prohibits persons who have receive one or more FISA Order(s) from making public
12 disclosures regarding the aggregate number of FISA Orders that such persons have received." In
13 response, Defendants identified "any provisions of any FISA order(s) received ... that require the
14 recipient not to reveal the existence of that order, to protect the secrecy of that order, or to
15 maintain any records concerning the acquisition or the aid furnished under that order"

16 Attached hereto as **Exhibit B** is a true and correct copy of an excerpt from Defendants'
17 Responses to Twitter's Second Set of Interrogatories.

18 7. I declare under penalty of perjury that the foregoing is true and correct.

19 Executed on April 29, 2019 at Palo Alto, CA.

20
21 /s/ Lee H. Rubin
LEE H. RUBIN

EXHIBIT A TO RUBIN DECLARATION

Pages 1 - 26

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

Before The Honorable Yvonne Gonzalez Rogers, Judge

TWITTER, INC.,)	
)	
Plaintiff,)	
)	
VS.)	NO. C 14-cv-04480 YGR
)	
MATTHEW G. WHITAKER, Acting)	
Attorney General of the United)	
States, et al.,)	
)	
Defendants.)	
_____)	

Oakland, California
Monday, November 26, 2018

TRANSCRIPT OF PROCEEDINGS

APPEARANCES:

For Plaintiff:

MAYER BROWN LLP
Two Palo Alto Square
3000 El Camino Real
Palo Alto, CA 94306-2112

BY: LEE H. RUBIN, ESQ.

MAYER BROWN LLP
71 South Wacker Drive
Chicago, IL 60606

BY: SAMANTHA C. BOOTH, ESQ.

(APPEARANCES CONTINUED ON FOLLOWING PAGE)

Reported By: Ana M. Dub, CSR No. 7445 RDR, CRR, CCRR, CRG, CCG
Official Reporter

APPEARANCES: (CONTINUED)

For Defendants:

UNITED STATES DEPARTMENT OF JUSTICE
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, DC 20001

BY: JULIA A. HEIMAN, ESQ.

Also Present:

Michele C. Lee, Esq., Twitter, Inc.

1 affidavit, perhaps write Your Honor a response of why we think
2 we agree with the Court's initial impression, and point out
3 where we think the deficiencies are, not only for Your Honor
4 but for the --

5 **THE COURT:** You keep talking about "we," but it should
6 be you.

7 **MR. RUBIN:** Oh, I'm sorry. I was just using a
8 universal --

9 **THE COURT:** I understand.

10 **MR. RUBIN:** It's only Lee Rubin, yeah.

11 **THE COURT:** And it's only me.

12 **MR. RUBIN:** I'm writing to you.

13 **THE COURT:** So, I mean, that's the way these things
14 work.

15 **MR. RUBIN:** Yeah. No, no. And I've done this before
16 several years ago, yeah. I know we sit in a skiff and I have a
17 secure computer; and whatever I can do to respond to it, I just
18 write to you and the Government, presumably.

19 The Government will obviously get to see what I -- if --
20 the way I had envisioned this procedure working is that if
21 the Court grants our access to the classified affidavit, I
22 would look at the affidavit. I would -- based upon my
23 understanding of the law and what I see, I would ask -- if I
24 don't have anything to say, I'll just look at it and look at
25 it.

1 But if I want to complete the record and let the Court
2 know why I believe that it's deficient under the governing
3 standard that this Court has articulated to justify this prior
4 restraint, I would put that in writing on a classified computer
5 and work with the appropriate DOJ security personnel to get
6 that to you.

7 And that would be our response that then would be part of
8 this record that Your Honor would consider, and then the
9 Ninth Circuit or any later court would consider, as our
10 position on the sufficiency or deficiencies of the classified
11 affidavit.

12 And then, if and when the time came that we looked at it,
13 we see how the privilege challenge turns out, and then we look
14 back at the classified logs and say there might be a small set
15 of discrete classified discovery that we'd also like to look
16 at. Then we would make that request.

17 But we don't think it's appropriate to make that request
18 now. It could lead to a lot of, from our vantage point,
19 unnecessary litigation about issues relating to the state
20 secret privilege that the Government has raised the specter of,
21 or other things, that really is not ripe.

22 Now, one thing I will say is that, you know, for the first
23 time -- and maybe Ms. Heiman can clarify this -- we had
24 known -- you know, the Government has said, I think, for the
25 past year that to the extent there's classified discovery or

CERTIFICATE OF REPORTER

I certify that the foregoing is a correct transcript
from the record of proceedings in the above-entitled matter.

DATE: Wednesday, December 5, 2018

Ana M. Dub

Ana M. Dub, CSR No. 7445, RMR, CRR, CCRR, CRG, CCG
U.S. Court Reporter

EXHIBIT B TO RUBIN DECLARATION

Attorneys for Defendants the Attorney General, et al.

1

1 **OBJECTION**

2 Defendants object to Interrogatory No. 4 as vague, overly broad, and unduly burdensome to the
3 extent that it does not specify an applicable time period for response. Defendants will provide
4 their response for the time period from the date of filing of the Second Amended Complaint,
5 ECF No. 114 (May 24, 2016) to the present.

6 **RESPONSE**

7 Subject to the above limitation and objections, and without waiving them, Defendants respond:
8 No.

9
10 **INTERROGATORY NO. 5:**

11 For any FISA court proceedings identified in response to Interrogatory No. 4, state:

- 12 i. The date such proceedings were commenced;
13 ii. The name(s) of the party or parties who initiated those proceedings; and
14 iii. The resolution of such proceedings (namely, whether any disclosure of aggregate
15 information more granular than that permitted under 50 U.S.C. § 1874(a)–(b) was
16 authorized).

17 **RESPONSE**

18 Subject to the above limitation and objections, and without waiving them, because there were no
19 proceedings identified pursuant to Interrogatory No. 4, Defendants do not respond to
20 Interrogatory No. 5.

21
22
23
24 **INTERROGATORY NO. 6:**

25 Identify the operative provision(s) of any statute, regulation, policy, procedure, order, or other
26 authority which You contend prohibits persons who have received one or more FISA Order(s)
27 from making public disclosures regarding the aggregate number of FISA Orders that such
28 persons have received.

OBJECTION

Defendants object to Interrogatory No. 6 on the grounds that it calls for legal conclusions. Defendants further object that Interrogatory No. 6 is vague and ambiguous and calls for speculation because it asks Defendants to speculate regarding the legal authority that may apply to a hypothetical situation, where the legal authority applicable may vary based on the specific information at issue. Among the authorities that might apply are, for example: Executive Order 13526, Sections 1.1–1.4, 2.1; 50 U.S.C. § 3605(a); any provisions of any FISA order(s) received by such persons that require the recipient not to reveal the existence of that order, to protect the secrecy of that order, or to maintain any records concerning the acquisition or the aid furnished under that order under security procedures approved by the Attorney General and the Director of National Intelligence; 50 U.S.C. § 1861(d), as to any order issued under FISA, Title V; 18 U.S.C. §§ 793, 794, 798; and any applicable nondisclosure agreement such a person may have signed.

INTERROGATORY NO. 7:

Identify the operative provision(s) of any statute, regulation, policy, procedure, order, or other unclassified authority which You contend limits the temporal scope of the prohibition (identified in Interrogatory No. 6) on public disclosures regarding aggregate FISA Orders received—that is, authority which would permit a recipient to disclose the specific, aggregate number of FISA Orders it received over a period of time after a specified time has passed since those FISA Orders were received—or, if no such authority exists, so state.

OBJECTION

Defendants object to Interrogatory No. 7 on the grounds that it calls for legal conclusions. Defendants further object that Interrogatory No. 7 is vague and ambiguous and calls for speculation because it asks Defendants to speculate regarding the legal authority that may apply to a hypothetical situation, where the legal authority applicable may vary based on the specific information at issue. For example, such authority may include Executive Order 13526, Sections 1.5, 2.1.

OBJECTION

Defendants object to the terms “systemic,” “overclassification,” and “improper” as vague and ambiguous. Defendants further object to Interrogatory No. 16 as unduly burdensome and oppressive insofar as it seeks information related to the activities of the entirety of the Legislative and Executive Branches. Defendants have limited their search to the components of the Department of Justice and Federal Bureau of Investigation reasonably likely to have information pertaining to Plaintiff’s request to publish aggregate data regarding its receipt of national security process. Defendants also object to identifying any such report to the extent such a classified report is protected from disclosure by the state secrets privilege, and the related statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

RESPONSE

Subject to the limitations and objections above, and without waiving them, Defendants respond that they are aware of no materials responsive to Interrogatory No. 16.

Dated: March 13, 2018

As to Objections,

CHAD A. READLER
Acting Assistant Attorney General

BRIAN STRETCH
United States Attorney

ANTHONY J. COPPOLINO
Deputy Branch Director

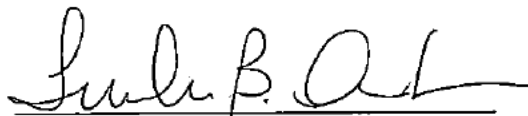
/s/ Julia A. Berman

JULIA A. BERMAN, Bar No. 241415
Senior Counsel
U.S. Department of Justice
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, D.C. 20044
julia.berman@usdoj.gov

Attorneys for Defendants

1
2 I, Trisha B. Anderson, declare under penalty of perjury that I am a Deputy General
3 Counsel in the Federal Bureau of Investigation, Office of the General Counsel, and based upon
4 information provided to me in my official capacity, the foregoing Responses to Plaintiff's
5 Second Set of Interrogatories are true and correct to the best of my knowledge and belief.
6

7 Executed this day of March 13th, 2018, pursuant to 28 U.S.C. § 1746.
8

9
10 

11 Trisha B. Anderson
12 Deputy General Counsel
13 Federal Bureau of Investigation
14 Office of the General Counsel
15
16
17
18
19
20
21
22
23
24
25
26
27
28

MAYER BROWN LLP
ANDREW JOHN PINCUS (*Pro Hac Vice*)
apincus@mayerbrown.com
1999 K Street, NW
Washington, DC 20006
Tel: (202) 263-3220 / Fax: (202) 263-3300

MAYER BROWN LLP
LEE H. RUBIN (SBN 141331)
lrubin@mayerbrown.com
DONALD M. FALK (SBN 150256)
dfalk@mayerbrown.com
SAMANTHA C. BOOTH (SBN 298852)
sbooth@mayerbrown.com
Two Palo Alto Square, Suite 300
3000 El Camino Real
Palo Alto, CA 94306-2112
Tel: (650) 331-2000 / Fax: (650) 331-2060

Attorneys for Plaintiff Twitter, Inc.

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION**

TWITTER, INC.,

Plaintiff,

v.

WILLIAM P. BARR, Attorney General of the
United States, *et al.*,

Defendants.

Case No. 14-cv-4480-YGR

**DECLARATION OF LINDA ISLEY IN
SUPPORT OF TWITTER, INC.'S
OPPOSITION TO DEFENDANTS'
INVOCATION OF STATE SECRETS
AND MOTION TO DISMISS**

I, Linda Isley, declare as follows:

1. I am a Global Senior Manager, Trust & Safety, for Plaintiff Twitter, Inc. ("Twitter"). I submit this declaration in support of Twitter's Opposition to Defendants' Invocation of State Secrets and Motion to Dismiss. Except as otherwise noted, I have personal knowledge of the facts stated in this declaration and if called as a witness, I could and would competently testify thereto.

2. I have been employed by Twitter since September 2018. During that period, my responsibilities have included managing the team which responds to legal process served on Twitter.

3. Based on my capacity as a Global Senior Manager, I am aware that Twitter has published 14 individual National Security Letters ("NSLs") dating back to 2009. These NSLs have generally been published as a result of the 2015 revisions to the NSL provisions permitting Twitter (and other recipients of NSLs) to challenge individual non-disclosure obligations issued in connection with NSLs.

4. Attached hereto as **Exhibit A** is a true and correct copy of an NSL issued on November 15, 2010, that was received by Twitter and that Twitter has since made public, with redactions.

5. Attached hereto as **Exhibit B** is a true and correct copy of an NSL issued on June 28, 2010, that was received by Twitter and that Twitter has since made public, with redactions.

6. Attached hereto as **Exhibit C** is a true and correct copy of an NSL issued on November 27, 2015, that was received by Twitter and that Twitter has since made public, with redactions.

7. I declare under penalty of perjury that the foregoing is true and correct.

Executed on April 29, 2019 at San Francisco, CA.

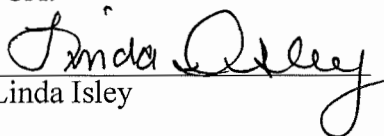

Linda Isley

EXHIBIT A TO ISLEY DECLARATION



U.S. Department of Justice

Federal Bureau of Investigation

In reply, Please refer to

File No. NSL-10-320727

2111 West Roosevelt Road
Chicago, IL 60608
November 15, 2010

Mr. Alec Macgillivray
General Counsel
Twitter
795 Folsom Street
Suite 600
San Francisco, CA 94107

Dear Mr. Macgillivray:

Under the authority of Executive Order 12333, dated July 30, 2008, and pursuant to Title 18 United States Code (U.S.C.), § 2709 (§ 201 of the Electronic Communications Privacy Act of 1986) (as amended), you are hereby directed to provide to the Federal Bureau of Investigation (FBI) the names, addresses, and length of service and electronic communications transactional records, to include existing transaction/activity logs and all electronic mail (e-mail) header information, for the below-listed email/IP address holder(s):

Accounts:	For Following Date(s) (YYYY-MM-DD):
[REDACTED]	For Current Subscriber

Please see the attachment following this letter for the types of information that you might consider to be a electronic communications transactional record. We are not directing that you should provide, and you should not provide, information pursuant to this letter that would disclose the content of any electronic communication. Title 18 United States Code § 2510(8) defines content as "any information concerning the substance, purport, or meaning of" a communication. Subject lines of e-mails and message content are content information and should not be provided pursuant to this letter.

If the time period noted above is from "inception," that term is intended to apply to the current account holder only. If the time period noted above is to the "present," that term is intended to direct production of information to the date of the processing of this letter.

Mr. Alec Macgillivray

If providing information to the date of processing is not feasible, please provide information to the date of receipt of this letter.

While fulfilling your obligations under this letter, please do not disable, suspend, lock, cancel or interrupt service to the above-described subscriber(s) or accounts. A service interruption or degradation may alert the subscriber(s)/account user(s) that investigative action is being taken. If you are not able to fulfill your obligations under this letter without alerting the subscriber/account user, please contact the FBI prior to proceeding.

In accordance with Title 18 U.S.C., § 2709(b), I certify that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, and that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States.

In accordance with Title 18 U.S.C. § 3511(c), an unlawful failure to comply with this letter, including any nondisclosure requirement, may result in the United States bringing an enforcement action.

You are directed to provide records responsive to this letter personally to a representative of the San Francisco Division within 5 business days of receipt of this letter. Please provide records in response to this letter in paper format or if possible, in electronic format. Due to security considerations, you should neither send the records through routine mail service nor non-secure fax, nor disclose the substance of this letter in any telephone conversation. In responding to this request in order to facilitate processing of the information, please reference the NSL-10-320727.

Any questions you have regarding this letter should be directed to the San Francisco Division or [REDACTED].

Your cooperation in this matter is greatly appreciated.

Sincerely,



Robert Grant

Special Agent In Charge
Chicago

Mr. Alec Macgillivray

ATTACHMENT

In preparing your response to this National Security Letter, you should determine whether your company maintains the following types of information which may be considered by you to be an electronic communications transactional record in accordance with Title 18 United States Code § 2709.

- Subscriber name and related subscriber information
- Account number(s)
- Date the account opened or closed
- Physical and or postal addresses associated with the account
- Subscriber day/evening telephone numbers
- Screen names or other on-line names associated with the account
- All billing and method of payment related to the account including alternative billed numbers or calling cards
- All e-mail addresses associated with the account to include any and all of the above information for any secondary or additional e-mail addresses and or user names identified by you as belonging to the targeted account in this letter
- Internet Protocol (IP) addresses assigned to this account and related e-mail accounts
- Uniform Resource Locator (URL) assigned to the account
- Plain old telephone(s) (POTS), ISDN circuit(s), Voice over internet protocol (VOIP), Cable modem service, Internet cable service, Digital Subscriber Line (DSL) asymmetrical/symmetrical relating to this account
- The names of any and all upstream and downstream providers facilitating this account's communications
- The above-listed information from "inception of the targeted account to the present" if this request cannot be processed as presently written

We are not directing that you should provide, and you should not provide, information pursuant to this letter that would disclose the content of any electronic communication. Title 18 United States Code § 2510(8) defines content as "any information concerning the substance, purport, or meaning of" a communication. Subject lines of e-mails are content information and should not be provided pursuant to this letter. If the records provided are particularly large we request that you provide this information in electronic format, preferably on a CD-ROM.

EXHIBIT B TO ISLEY DECLARATION

Routine

U.S. Department of Justice

Federal Bureau of Investigation

In reply, Please refer to

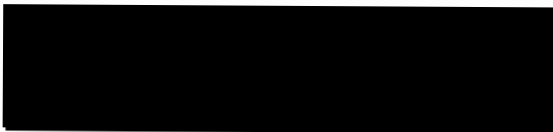
File No. NSL-10-293548

601 Fourth Street NW
 Washington, DC 20535-0002
 June 28, 2010

Mr. Alec Macgillivray
 General Counsel
 Twitter
 795 Folsom Street
 Suite 600
 San Francisco, CA 94107

Dear Mr. Macgillivray:

Under the authority of Executive Order 12333, dated July 30, 2008, and pursuant to Title 18 United States Code (U.S.C.), § 2709 (§ 201 of the Electronic Communications Privacy Act of 1986) (as amended), you are hereby directed to provide to the Federal Bureau of Investigation (FBI) the names, addresses, and length of service and electronic communications transactional records, to include existing transaction/activity logs and all electronic mail (e-mail) header information, for the below-listed email/IP address holder(s):



Accounts:	For Following Date(s) (YYYY-MM-DD):
[Redacted]	From Inception to Present

Please see the attachment following this letter for the types of information that you might consider to be a electronic communications transactional record. We are not directing that you should provide, and you should not provide, information pursuant to this letter that would disclose the content of any electronic communication. Title 18 United States Code § 2510(8) defines content as "any information concerning the substance, purport, or meaning of" a communication. Subject lines of e-mails and message content are content information and should not be provided pursuant to this letter.

Mr. Alec Macgillivray

If the time period noted above is from "inception," that term is intended to apply to the current account holder only. If the time period noted above is to the "present," that term is intended to direct production of information to the date of the processing of this letter. If providing information to the date of processing is not feasible, please provide information to the date of receipt of this letter.

While fulfilling your obligations under this letter, please do not disable, suspend, lock, cancel or interrupt service to the above-described subscriber(s) or accounts. A service interruption or degradation may alert the subscriber(s)/account user(s) that investigative action is being taken. If you are not able to fulfill your obligations under this letter without alerting the subscriber/account user, please contact the FBI prior to proceeding.

In accordance with Title 18 U.S.C., § 2709(b), I certify that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, and that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States.

In accordance with Title 18 U.S.C. § 2709(c)(1), I certify that a disclosure of the fact that the FBI has sought or obtained access to the information sought by this letter may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of a person. Accordingly, Title 18 U.S.C. § 2709(c)(1) and (2) prohibits you, or any officer, employee, or agent of yours, from disclosing this letter, other than to those to whom disclosure is necessary to comply with the letter or to an attorney to obtain legal advice or legal assistance with respect to this letter.

In accordance with Title 18 U.S.C. § 2709(c)(3), you are directed to notify any persons to whom you have disclosed this letter that they are also subject to the nondisclosure requirement and are therefore also prohibited from disclosing the letter to anyone else.

In accordance with Title 18 U.S.C. § 2709(c)(4), if the FBI asks for the information, you should identify any person to whom such disclosure has been made or to whom such disclosure will be made. In no instance will you be required to identify any attorney to whom disclosure was made or will be made in order to obtain legal advice or legal assistance with respect to this letter.

In accordance with 18 U.S.C. § 3511(a) and (b)(1), you have a right to challenge this letter if compliance would be unreasonable, oppressive, or otherwise unlawful.

Mr. Alec Macgillivray

You also have the right to challenge the nondisclosure requirement set forth above. If you wish to make a disclosure that is prohibited by the nondisclosure requirement, you must notify the FBI, in writing, of your desire to do so within 10 calendar days of receipt of this letter. That notice must be mailed or faxed to the Washington Field Office, attention: [REDACTED] with a copy to FBI HQ, attention: General Counsel (fax number: 202-324-5366) and must reference the date of the NSL and the identification number found on the upper left corner of the NSL. If you send notice within 10 calendar days, the FBI will initiate judicial proceedings in approximately 30 days in order to demonstrate to a federal judge the need for nondisclosure and to obtain a judicial order requiring continued nondisclosure. The nondisclosure requirement will remain in effect unless and until there is a final court order holding that disclosure is permitted.

If you do not send notice of your desire to disclose the NSL or the fact that you produced records in response to it within 10 calendar days of receipt, then the nondisclosure provision will remain in effect, subject to your opportunity to make an annual challenge to the nondisclosure requirement as provided by subsection 3511(b).

In accordance with Title 18 U.S.C. § 3511(c), an unlawful failure to comply with this letter, including any nondisclosure requirement, may result in the United States bringing an enforcement action.

You are directed to provide records responsive to this letter personally to a representative of the San Francisco Division within 10 business days of receipt of this letter. Please provide records in response to this letter in paper format or if possible, in electronic format. Due to security considerations, you should neither send the records through routine mail service nor non-secure fax, nor disclose the substance of this letter in any telephone conversation. In responding to this request in order to facilitate processing of the information, please reference the NSL-10-293548.

Mr. Alec Macgillivray

Any questions you have regarding this letter should be directed to the San Francisco Division or [REDACTED].

Your cooperation in this matter is greatly appreciated.

Sincerely,

John G. Perren
Special Agent In Charge
Washington Field Office

Mr. Alec Macgillivray

ATTACHMENT

In preparing your response to this National Security Letter, you should determine whether your company maintains the following types of information which may be considered by you to be an electronic communications transactional record in accordance with Title 18 United States Code § 2709.

- Subscriber name and related subscriber information
- Account number(s)
- Date the account opened or closed
- Physical and or postal addresses associated with the account
- Subscriber day/evening telephone numbers
- Screen names or other on-line names associated with the account
- All billing and method of payment related to the account including alternative billed numbers or calling cards
- All e-mail addresses associated with the account to include any and all of the above information for any secondary or additional e-mail addresses and or user names identified by you as belonging to the targeted account in this letter
- Internet Protocol (IP) addresses assigned to this account and related e-mail accounts
- Uniform Resource Locator (URL) assigned to the account
- Plain old telephone(s) (POTS), ISDN circuit(s), Voice over internet protocol (VOIP), Cable modem service, Internet cable service, Digital Subscriber Line (DSL) asymmetrical/symmetrical relating to this account
- The names of any and all upstream and downstream providers facilitating this account's communications
- The above-listed information from "inception of the targeted account to the present" if this request cannot be processed as presently written

We are not directing that you should provide, and you should not provide, information pursuant to this letter that would disclose the content of any electronic communication. Title 18 United States Code § 2510(8) defines content as "any information concerning the substance, purport, or meaning of" a communication. Subject lines of e-mails are content information and should not be provided pursuant to this letter. If the records provided are particularly large we request that you provide this information in electronic format, preferably on a CD-ROM.

EXHIBIT C TO ISLEY DECLARATION



Federal Bureau of Investigation

In reply, Please refer to

File No. NSL-15-419074

Los Angeles Division
FOB, Suite 1700
11000 Wilshire Boulevard
Los Angeles, CA 90024
November 27, 2015

Ms. Vijaya Gadde
General Counsel
Twitter
1355 Market Street, Suite 900
San Francisco, CA 94102
[REDACTED]

Dear Ms. Gadde:

Pursuant to Title 18, United States Code (U.S.C.), Section 2709 (Section 201 of the Electronic Communications Privacy Act of 1986), to the extent you provide an electronic communication service as defined in 18 U.S.C. § 2510(15), you are hereby directed to produce to the Federal Bureau of Investigation (FBI) the name, address, and length of service for all services, as well as all accounts, provided to the individual(s) or identifier(s) listed below:

Account:	For Following Date(s) (YYYY-MM-DD):
[REDACTED]	From Inception to Present

If the period noted above is from "inception," that term applies to the current account holder only. If the period noted above is to the "present," that term directs production of information to the date you process this letter.

While fulfilling your obligations under this letter, please do not disable, suspend, lock, cancel, or interrupt service to the above-described subscriber(s) or accounts. A service interruption or degradation may alert the subscriber(s) and account users(s) to the investigative action. If you are not able to fulfill your obligations under this letter without alerting the subscriber(s) and account user(s), please contact the FBI prior to proceeding.

In accordance with 18 U.S.C. § 2709(b), I certify the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, and such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States.

NONDISCLOSURE PROVISIONS

In accordance with 18 U.S.C. § 2709(c)(1), I certify disclosure of the fact the FBI has sought or obtained access to the information or records sought by this letter may result in a danger to the national security of the United States; interference with a criminal, counterterrorism, or counterintelligence investigation; interference with diplomatic relations; or danger to the life or physical safety of any person, that is related to an authorized investigation to protect against international terrorism or clandestine intelligence activities.

In accordance with 18 U.S.C. §§ 2709(c)(1)-(2), you, any officer, employee, or agent of yours are prohibited from disclosing this letter or disclosing that the FBI has sought or obtained access to information, other than to those to whom disclosure is necessary to comply with the letter or to an attorney to obtain legal advice or legal assistance with respect to this letter.

In accordance with 18 U.S.C. § 2709(c)(3), you are directed to notify any persons to whom you have disclosed this letter that they are also subject to the nondisclosure requirement and are therefore also prohibited from disclosing the letter to anyone else.

In accordance with 18 U.S.C. § 2709(c)(4), if the FBI asks for the information, you should identify any person to whom such disclosure has been made or to whom such disclosure will be made. In no instance will you be required to identify any attorney to whom disclosure was made or will be made in order to obtain legal advice or legal assistance with respect to this letter.

In accordance with 18 U.S.C. §§ 3511(a)-(b)(1), you have a right to challenge this letter if compliance would be unreasonable, oppressive, or otherwise unlawful. You also have the right to challenge the nondisclosure requirement set forth above. If you wish to make a disclosure prohibited by the nondisclosure requirement, you must notify the FBI, in writing, of your desire to do so within 10 calendar days of receipt of this letter. The notice must be mailed or faxed to the Los Angeles Division, attention: [REDACTED] and a copy faxed to FBI HQ, attention: General Counsel (fax number 202-324-5366). Your notice must reference the date of this letter and the File Number listed on the upper left corner of this letter. If you

send notice within 10 calendar days of receipt of this letter, the FBI will initiate judicial proceedings in approximately 30 days in order to demonstrate to a federal judge the need for nondisclosure and to obtain a judicial order requiring continued nondisclosure. The nondisclosure requirement will remain in effect unless and until there is a final court order holding that disclosure is permitted.

If you do not send notice of your desire to disclose the NSL or the fact you produced records in response to it within 10 calendar days of receipt, then the nondisclosure provision will remain in effect, subject to your opportunity to make an annual challenge to the nondisclosure requirement as provided by 18 U.S.C. § 3511(b).

GUIDANCE ON RESPONDING TO THE FBI

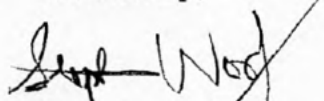
In accordance with 18 U.S.C. § 3511(c), an unlawful failure to comply with this letter, including any nondisclosure requirement, may result in the United States bringing an enforcement action.

You are directed to provide electronically the records responsive to this letter within 21 business days of receipt of this letter to the FBI's Operational Technology Division (OTD). If you have questions about this request, you may contact [REDACTED] or an OTD representative.

Due to security considerations, you should NOT disclose the substance of this letter in any telephone conversation. When responding to this letter, please refer to File No. NSL-15-419074.

Your cooperation in this matter is greatly appreciated.

Sincerely,



Stephen Woolery
Special Agent in Charge
Los Angeles